

REMARKS

Applicants respectfully request that the above-identified application be reexamined.

Claims 1-29 are pending in this application. The Office Action mailed September 24, 2007 (hereinafter "Office Action"), rejected Claims 2-4, 6, 7, 16, 17, 20-22, 24, and 25 under 35 U.S.C. § 112, second paragraph, as using a trademark to identify or describe a particular product. Claims 1-8, 10-12, 14-26, 28, and 29 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Application Publication No. 2002/0143961, to Siegel et al. (hereinafter "Siegel et al."). Claims 9, 13, and 27 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Siegel et al. in view of U.S. Patent No. 6,370,141, issued to Giordano III et al. (hereinafter "Giordano III et al.").

Pursuant to 37 C.F.R. § 1.111 and for the reasons set forth below, applicants respectfully request reconsideration and allowance of the pending claims. Prior to discussing in detail why applicants believe that all the claims in this application are allowable, a brief description of the disclosed subject matter and brief descriptions of the teachings of the cited and applied references are provided. The following descriptions of the disclosed subject matter and the cited and applied references are not provided to define the scope or interpretation of any of the claims of this application. Instead, these descriptions are provided solely to assist the United States Patent and Trademark Office in recognizing the differences between the pending claims and the cited references, and should not be construed as limiting on the disclosed subject matter.

Disclosed Subject Matter

A system and method that provide a user choice setting process that permits applications to safely modify user choice settings in a manner that is verifiable and transparent to the user is disclosed. The system and method operate to advantageously enforce and protect user choice settings and to deter applications from modifying those settings without explicit user approval.

User choice settings are stored as protected values. Applications request modifications to the user choice settings by calling the user choice setting process to obtain approval from the user. Upon receiving approval, the user choice setting process first modifies the corresponding access control indicator of the protected value to allow the user to write the value. Once the

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINNESS^{PLLC}
1420 Fifth Avenue, Suite 2800
Seattle, Washington 98101
206 682.8100

corresponding access control indicator of the protected value has been modified, the user choice setting process is able to modify the user choice setting as requested. Before returning control of the protected value to the system, the user choice setting process restores the corresponding access control indicator to again only allow the user to read but not write the newly modified protected value. Preferably, the user choice setting process generates an approval user interface to display to the user their user choice settings, and to receive from the user an input to approve the application's request to change those settings. Should the user not approve the application's request, the user choice setting process terminates the request and does not modify the corresponding access control indicator of the protected value, nor does it modify the protected value.

Summary of Siegel et al. (U.S. Patent Application Publication No. 2002/0143961)

Siegel et al. is purportedly directed toward a customer profile access protocol with flexible access control capabilities. The protocol facilitates secure and privacy enabled access to user profile data. The user profile data may be accessed by clients, such as other users, service providers and system administrators. The user profile data is used by service providers and system administrators. The user profile data is used by service providers to customize services provided to users. Permissions that control profile access are established under user control. The user specifies different permissions for different grains of information within the user profile. Clients may be grouped such that permissions may be associated with a single group or combinations of groups specified by algebraic set operators. While Siegel et al. describes a method of facilitating access to user profile data, it fails to teach applications requesting modifications to user choice settings and modifying user choice setting in response to user authorization.

Summary of Giordano III et al. (U.S. Patent No. 6,370,141)

Giordano III et al. is purportedly directed toward a method of changing the settings of an Internet appliance using the Internet. An Internet appliance accesses an HTML page on a Web site containing configuration information for an Internet appliance, such as an Internet compatible telephone. Data from the HTML page are downloaded to the Internet appliance to

modify its options or settings automatically upon accessing the HTML page, or as directed by the user. The data is downloaded to a programmable memory in the Internet appliance and the stored data is used to upgrade the Internet appliance. The upgrade HTML page includes information to alert the user when new information is available regarding changes to options and settings of the Internet appliance.

Rejection of Claims 2-4, 6, 7, 16, 17, 20-22, 24, and 25 Under 35 U.S.C. § 112, Second Paragraph

As indicated above, Claims 2-4, 6, 7, 16, 17, 20-22, 24, and 25 were rejected under 35 U.S.C. § 112, second paragraph, as using a trademark to identify or describe a particular product. Applicants have amended the above claims by deleting the Windows® trademark from the claims and by replacing the Windows trademark with the term "operating system" and related terminology where appropriate. Applicants respectfully submit that amended Claims 2-4, 6, 7, 16, 17, 20-22, 24, and 25 now comply with requirements of 35 U.S.C. § 112, second paragraph, and thus this rejection has been rendered moot and should be withdrawn.

Rejection of Claims 1-8, 10-12, 14-26, 28, and 29 Under 35 U.S.C. § 102(b)

As indicated above, Claims 1-8, 10-12, 14-26, 28, and 29 were rejected under 35 U.S.C. § 102(b) as being anticipated by Siegel et al.

Claims 1-8, 10-11, 19-26, 28, and 29

Remarks accompanying the rejection of independent Claims 1 and 19 in the Office Action state:

As per claims 1 and 19, Siegel discloses storing a user choice setting as a protected value that is secured by an access control indicator (Siegel, Paragraph 0004 00039, user permissions stored in a database with modification settings, use of passwords protect an account) receiving an input from a user authorizing an application to modify the user choice setting on the user's behalf (Siegel, Paragraph 0026, user needs to be authenticated prior to the modification of a profile), modifying the access control indicator to permit writing to the protected value, modifying the user choice setting by writing a modified user choice setting to the protected value (Siegel, Paragraph 0026, once a party whether the user or administrator is verified or authenticated, changes to the settings maybe

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLC}
1420 Fifth Avenue, Suite 2800
Seattle, Washington 98101
206 682 8100

[sic] made thus taking a way [sic] any protection indicators), and restoring the access control indicator to prevent writing to the protected value (Siegel, 0026, inherent that once a user or administrator is done modifying the profile the user or administrator will log out and the profile will be protected from modifications until another party is verified and authenticated).

Claim 1, as amended, recites as follows:

1. A method for controlling modifications to user choice settings, the method comprising:

(a) storing a user choice setting as a protected value that is secured by an access control indicator; **the user choice setting determining an application's operation in a user's computing device, the application's operation including handling a particular event in the user's computing device;**

(b) **in response to receiving a request from the application to modify the user choice setting, requesting authorization from the user to modify the user choice setting; and**

(c) **in response to** receiving an input from a user authorizing the application to modify the user choice setting on the user's behalf:

(i) modifying the access control indicator to permit writing to the protected value;

(ii) modifying the user choice setting by writing a modified user choice setting to the protected value; and

(iii) restoring the access control indicator to prevent writing to the protected value. (Emphasis added.)

Applicants respectfully submit that Claim 1, as amended, is not anticipated by Siegel et al. Initially, applicants respectfully disagree with the Office Action that Siegel et al. discloses "receiving an input from a user authorizing an application to modify the user choice setting on the user's behalf" clause of Claim 1 prior to the present amendment. Paragraph [0026] of Siegel et al., referenced by the Office Action with regard to this clause, states only that a "verified and authenticated user" may "review and modify the users user profile and associated permissions." The referenced paragraph further describes the interface via which the user may communicate with the PMT server, for example, a web page that allows the user to modify his profile and permissions. Thus, it is the user who can access his profile and security settings in order to modify them. Nowhere in the referenced paragraph or elsewhere does Siegel et al. disclose, teach, or remotely suggest that an application may modify the settings on a user's behalf based

upon the user's permission, as now more clearly recited in Claim 1, as amended. Furthermore, nowhere does Siegel et al. describe or suggest that an application may request the modification of a user choice setting. Indeed, the clients that request to access the user information in Siegel et al. are only users, administrators, and service providers, not applications. (Paragraph [0019].)

Applicants further point out that the method described in Siegel et al. is different in principle than the one recited in amended Claim 1. Siegel et al. describes a method wherein the clients or the groups of clients do not request special permission from a user to access the information in the user profile; instead, they access the user information according to the permissions associated with groups or individual clients that specify the type of access, e.g., write, read, delete, or permission write access. (Paragraphs [0032], [0033].) In contrast, Claim 1 recites a method which requires a user's direct involvement, namely, permission or denial, each time an application requests to change a user choice setting which is a protected value. Thus, Siegel et al. fails to teach, disclose, or remotely suggest the "requesting authorization from the user to modify the user choice setting" and the "receiving an input from a user" clauses of Claim 1, as amended.

In order to better distinguish Claim 1 from Siegel et al., applicants have amended Claim 1 to include the "in response to a request from the application to modify the user choice setting" recitation, as well as the clause reciting that "the user choice setting" determines "an application's operation in a user's computer, wherein the application's operation includes handling a particular event in the user's computer." For the reasons described above, applicants submit that Claim 1 is not anticipated by Siegel et al., and is thus allowable. Claims 2-8, 10, and 11, which depend directly or indirectly from Claim 1, are also submitted to be allowable for at least the reasons why Claim 1 is submitted to be allowable.

With regard to independent Claim 19, the applicants refer to the rationale provided in the above discussion of Claim 1 with respect to the clause "receive an input from a user authorizing an application to modify the user choice setting on the user's behalf." In order to better

distinguish Claim 19 from Siegel et al., applicants have amended Claim 19 with the same subject matter as the subject matter added to Claim 1, namely, with the "in response to a request from an application to modify the user choice setting" recitation, as well as with the clause reciting that "the user choice setting" determines "an application's operation in a user's computer, wherein the application's operation includes handling a particular event in the user's computer." As a result, applicants respectfully submit that Claim 19 is not anticipated by Siegel et al. and thus is allowable. Claims 20-26, 28, and 29, which depend directly from Claim 19, are also submitted to be allowable for at least the reasons why Claim 19 is submitted to be allowable.

Claims 12 and 14-18

Remarks accompanying the rejection of independent Claim 12 in the Office Action state:

As per claim 12, Siegel discloses a registry for storing a user choice setting as a protected value in a registry key (Siegel, Paragraph 0004, database with list of authorized users and their settings, protected by the permissions in the database) an access control list (ACL) for securing the registry key (Siegel, Paragraph 0004, database with list of authorized users to access data in the network), an interface to control modifications to the user choice setting (Siegel, Paragraph 0026, interface for user to modify settings) and an application issuing a request to modify the user choice setting via the interface (Siegel, Paragraph 0026, interface for user to modify settings), the interface obtaining an approval of the request from a user (Siegel, Paragraph 0026, user must be verified and authenticated prior to setting modifications) the interface further modifying the ACL to permit writing to the protected value in the registry key upon obtaining the approval, the interface further writing to the protected value in the registry key upon obtaining the approval, the interface further writing to the protected value the modified user choice setting Siegel, Paragraph 0026, interface for user to modify settings), and the interface further restoring the ACL to prevent writing to the protected value in the registry key after writing the modified user choice setting (Siegel, 0026, inherent that once a user or administrator is done modifying the profile the user or administrator will log out and the profile will be protected from modifications until another party is verified and authenticated).

As amended, Claim 12 recites as follows:

12. A system for communicating user choice settings between an application and a registry for storing the user choice settings, the system comprising:

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue, Suite 2800
Seattle, Washington 98101
206.682.8100

a registry for storing a user choice setting as a protected value in a registry key, **the user choice setting determining an application's operation in a user's computing device, the application's operation including handling a particular event in the user's computing device;**
an access control list (ACL) for securing the registry key;
an interface to control modifications to the user choice setting; and
the application issuing a request to modify the user choice setting on the user's behalf via the interface, the interface obtaining an approval of the request from a user; the interface further modifying the ACL to permit writing to the protected value in the registry key upon obtaining the approval, the interface further writing to the protected value the modified user choice setting; and the interface further restoring the ACL to prevent writing to the protected value in the registry key after writing the modified user choice setting. (Emphasis added.)

Applicants respectfully submit that Claim 12, as amended, is not anticipated by Siegel et al. Specifically, applicants respectfully disagree with the Office Action that Siegel et al. discloses the "application issuing a request to modify the user choice setting via the interface" clause of Claim 12. As discussed above with regard to Claim 1, paragraph [0026] of Siegel et al., referenced by the Office Action with regard to this clause, states only that a "verified and authenticated user" may "review and modify the users user profile and associated permissions." The referenced paragraph further describes the interface via which the user may communicate with the PMT server, such as a web page that allows the user to modify his profile and permissions. However, as discussed above, nowhere does Siegel et al. describe "the application issuing a request to modify the user choice setting." Indeed, the clients that request to access the user information in Siegel et al. are only users, administrators, and service providers, not applications. (Paragraph [0019].)

In order to better distinguish Claim 12 from Siegel et al., applicants have amended Claim 12 to include the clause containing the same subject matter as amended Claims 1 and 19, namely, specifying that "the user choice setting" determines "an application's operation in a user's computer, wherein the application's operation includes handling a particular event in the user's computer." Applicants have further amended the last clause of Claim 12 to recite that an application issues a request to modify user settings "on user's behalf." Applicants refer to the

rationale provided in the above discussion of Claim 1 with respect to the clause "receive an input from a user authorizing an application to modify the user choice setting on the user's behalf." As a result, applicants respectfully submit that Claim 12 is not anticipated by Siegel et al. and thus is allowable. Claims 14-18, which depend directly from Claim 19, are also submitted to be allowable for at least the reasons why Claim 19 is submitted to be allowable.

Rejection of Claims 9, 13, and 27 Under 35 U.S.C. § 103(a)

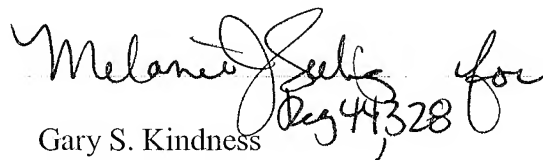
As indicated above, Claims 9, 13, and 27 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Siegel et al. in view of Giordano III et al. Claim 9 depends from Claim 1, Claim 13 depends from Claim 12, and Claim 27 depends from Claim 19 and are submitted to be allowable for at least the same reasons as discussed above with regard to Claims 1, 12, and 19. Giordano III et al. does not disclose or suggest the differences of Siegel et al. as discussed above.

CONCLUSION

In view of the amendments and remarks above, applicants respectfully submit that the pending claims are in condition for allowance. Reconsideration and reexamination of the application and allowance of the claims at an early date are solicited. If the Examiner has any questions or comments concerning the foregoing response, the Examiner is invited to contact the applicants' undersigned attorney at the number below.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLLC}

 for
Reg 47328

Gary S. Kindness
Registration No. 22,178
Direct Dial No. 206.695.1702

GSK/VXR:tmm